TECHNOLOGY

Cryptojacking on the rise in poorer countries where ransoms can't be paid

Criminals are finding ways to turn user's computers into cryptominers. (Pixabay)

Patrick Howell O'Neill Nov 27, 2017 | CyberScoop

A collection of poorer countries in Eastern Europe are the only places in cyberspace where ransomware isn't seen as a top threat.

still connected to the internet.

Rich countries like the United States are ripe for ransomware because the population has more money to pay ransoms, with the practice becoming a $2 billion criminal industry in 2017. Knowing that residents in less-developed countries are less likely be able to pay ransoms, criminals are heavily targeting poorer regions with malware that uses victims' computers to mine cryptocurrency — a scheme known as cryptomining or cryptojacking — according to new research from the cybersecurity firm Bitdefender.

"Ransomware is the number one infection globally," Bogdan Botezatu, the senior threat analyst at the cybersecurity firm Bitdefender, told CyberScoop. "Cryptominers rank second."

Cryptojacking software is the most common infection in Ukraine, Bulgaria, Romania and Greece, according to telemetry data from Bitdefender's security products, which have 500 million users. Cryptojackers are progressively moving away from bitcoin and toward newer cryptocurrencies like Monero and Zcash, which are both easier to mine and offer more anonymity than bitcoin.

Targeting of Eastern European countries echoes research from earlier this year that showed a criminal's profit when it comes to ransomware depends on the ability and willingness of the victim to pay. Economists came up with a more much sophisticated model than anything currently being used by criminals but the basic idea still applies: To maximize profit, you have to know your victim. For that reason, a mass of hackers decided cryptojackers are the best way to take money from Eastern Europeans who can't pay ransom rates seen in wealthier countries.

"We have seen an increase in cryptominers over the last year," Trend Micro's vice president of cloud research Mark Nunnikhoven said. "The biggest shift has been in malware using the resources of an infected endpoint to generate cryptocurrency."

Cryptominers can be used legally when website owners ask visitors for permission to use their processing power for mining, mainly as a way to pay for the site's operation. The practice turns definitively abusive when miners access and use other people's machines without permission.

The biggest impact is that illicit cryptominers are denying people access to their computer's resources, Nunnikhoven explained. The software slows down a target's computer by siphoning off memory and processing power while also driving up unsuspecting users' electricity and data bills.

Some of these costs are small. When you spread the hacking campaign out to thousands of devices, however, the vast amount of computing power can bring in a wealth of cryptocurrency.

Websites like The Pirate Bay, Showtime and Politifact have all been used to launch cryptominers either by the website's owner or hackers who placed the code there secretly for their own benefit. Recent research found 2,500 websites currently engaged in cryptojacking.

As cybercriminals turn increased attention to cryptominers, the malware is expected to proliferate and become more sophisticated in the coming year.

Just days after the exposure of EternalBlue and EternalRomance exploits, allegedly originating from the NSA, the Monero miner Adylkuzz was used to infect computers around the same time that WannaCry ransomware exploded.

It's relatively easy to calculate the total money earned by ransomware but cryptominers, by contrast, present a challenge because it depends on how long the malware can persist on the machine.

In addition to specific regions of the world, hackers have zeroed in on gamers who run relatively powerful machines that have all the necessary hardware to make big money mining cryptocurrency.

"These gamers have good rigs with state of the art graphics cards," Botezatu said. Graphics cards are ideal to handle big tasks like cryptocurrency mining. "They are very reluctant to run antivirus solutions because that induces lag and performance loss. They want to enjoy the full gaming experience. No wonder most cryptominers are actually delivered via cracks, pirated copies of cheats. It's very easy for someone like this to get infected. I presume [the hackers] are making a lot of money."

It's more and more common to hijack vulnerable websites and install cryptominers so that visitors are infected.

Often the website owners themselves will insert cryptominers that operate without user permission. Pirate websites that, for instance, illegally stream video are commonly laced with cryptominers which supplements the owner's income in addition to advertisements. An entire ecosystem of websites illegally streaming sports leagues like the National Basketball Association or the English Premiere League now rely heavily on cryptominers to produce revenue.

Google is considering options to block illicit cryptomining in its Chrome web browser. A Chrome extension called No Coin blocks abusive mining.

Cryptominers are so easy and prolific that a wide range of hacking groups have taken them up. There is no central group or even world region to pinpoint as a single source.

“We thought maybe cryptomining originated in the former Soviet Union,” Botezatu said. “But it’s not. We realized cryptomining fraud happens everywhere.”

-In this Story-

cryptocurrency, cryptojacking, google chrome, Monero, ransomware, Zcash

RELATED NEWS

TECHNOLOGY

Equifax says 2.4 million...

by **Patrick Howell O'Neill** • 2 days ago

FINANCIAL

Big banks want to weaken...

by **Patrick Howell O'Neill** • 3 days ago

GOVERNMENT

DHS leaders push...

by **Chris Bing** • 3 days ago